Craig A. Hansen (SBN 209622)
Email: craig@hansenlawfirm.net
Sarah Wager (SBN 209277)
Email: sarah@hansenlawfirm.net
Bruno Tarabichi (SBN 215129)
Email: bruno@hansenlawfirm.net
HANSEN LAW FIRM, P.C.
75 E. Santa Clara Street, Suite 1150
San Jose, CA 95113
Telephone: (408) 715-7980
Facsimile: (408) 715-7001

Attorneys for Plaintiff
My Choice Software, LLC,
a California limited liability company

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

My Choice Software, LLC, a California limited liability company,

Plaintiff,

v.

TaskUs, Inc. a Delaware corporation; Tassilo Heinrich, an Individual; Shopify, Inc.; Shopify Holdings (USA), Inc.; Shopify (USA) Inc.; and DOES 1-50, inclusive,

Defendants.

Case No. 8:22-cv-01710-DOC-DFM

PLAINTIFF MY CHOICE SOFTWARE, LLC'S FIRST AMENDED COMPLAINT FOR:

(1) BREACH OF CONTRACT
(2) BREACH OF THIRD PARTY CONTRACT
(3) VIOLATION OF THE CFAA
(4) VIOLATION OF THE CFAA
(5) VIOLATION OF CDAFA
(6) VIOLATION OF CDAFA
(7) NEGLIGENCE
(8) NEGLIGENCE
(9) CONVERSION
(10) RECEIPT OF STOLEN PROPERTY
(11) UNJUST ENRICHMENT

DEMAND FOR JURY TRIAL

Plaintiff My Choice Software, LLC ("MCS" or "Plaintiff"), by and through its attorneys, brings this case in the Central District of California pursuant to 28 U.S.C. §§ 1331, and 1367, as this action involves claims arising under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 and contains related California state law claims. For its First Amended Complaint in this action, Plaintiff alleges:

THE PARTIES

1. MCS is a California limited liability company with its principal place of business in Lake Forest, California.

2. Defendant TaskUs, Inc. ("TaskUs") is a Delaware corporation with its principal place of business at 1650 Independence Drive, Suite 100, New Braunfels, Texas 78132. TaskUs is registered with the California Secretary of State and was headquartered in Santa Monica, California.

3. Defendant Tassilo Heinrich ("Heinrich") is an individual who resides in Orange County, California.

4. Defendant Shopify, Inc. ("Shopify") is a Canadian Corporation with offices at 151 O'Connor Street, Ground Floor, Ottowa, Ontario K2P 2L8.

5. Defendant Shopify Holdings (USA), Inc. ("Shopify Holdings") is a Delaware corporation with its principal place of business in the United States. Shopify Holdings (USA), Inc. acts as a holding company for all of Shopify Inc.'s U.S.-based subsidiaries.

6. Defendant Shopify (USA) Inc. ("Shopify USA") is a Delaware corporation registered with the California Secretary of State. It is a wholly owned subsidiary of Shopify, Inc.

7. Upon information and belief, Shopify Holdings and Shopify USA are the functional equivalents of Shopify, Inc. because the three entities make no distinction between themselves in the public eye and use the same logos, trademarks, and websites, making it impossible to know the extent of any of the

Shopify entities' involvement in this data breach. Shopify, Inc., Shopify Holdings (USA), Inc., and Shopify (USA) Inc. are referred herein to as the "Shopify Defendants."

8. Each of the defendants has participated in and is in some manner responsible for the acts described in this Complaint and the damage resulting therefrom. Plaintiff is informed and believes, and based thereon alleges, that defendants acts as agents, employees, supervisors, partners, conspirators, servants and/or joint venturers of each other, and in doing the acts hereafter alleged, were acting within the scope and authority of such agency, employment, partnership, conspiracy, enterprise and/or joint venture, and with the express and/or implied permission, knowledge, consent, authorization and ratification of their co-defendants.

9. MCS is ignorant of the true names of the other defendants sued herein as Does 1–50, inclusive, and therefore, sues these Doe defendants by such fictitious names. The Doe defendants are likely to include, among others, any additional individuals who directed, authorized, or participated in the unlawful conduct described in this Complaint, including two unknown employees of TaskUs. MCS will amend this Complaint to allege their true names and capacities when ascertained.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction of this action under 28 U.S.C. §§ 1331, and 1367, as this action involves claims arising under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, combined with related and supplemental state law claims.

11. Defendants are subject to personal jurisdiction in this district because defendant TaskUs and the Shopify Defendants conduct substantial, continuous, and systematic activities in this judicial district, because defendant Heinrich resides in Orange County, California, and because MCS's causes of action contained herein

arise out of or result from defendants' contacts with this judicial district, including defendant Heinrich unlawfully accessing and/or providing a means for others to access MCS's protected computer and data remotely from Orange County, California.

12. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(a) because Defendant Heinrich resides in this judicial district. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims occurred in this judicial district.

FACTS RELEVANT TO ALL CLAIMS

The Shopify Defendants and Their Contacts with the U.S. and California

13. Shopify is an e-commerce platform for online stores that offers services to online merchants, including payments, marketing, shipping, and customer engagement tools.

14. According to its 2023 Annual Report, Shopify derives 66.4% of its revenue from sales in the United States ($3,719,489,000), whereas only 6.2% of its revenue is derived from sales in Canada ($345,915,000).

15. On information and belief, Shopify's sales revenue from California exceeds the revenue from any other U.S. state.

16. According to its 2023 Annual Report, Shopify "has office, commercial and warehouse leases" in the United States. On information and belief, this includes California.

17. Shopify also has a location called "Shopify Los Angeles" located at 777 South Alameda, Building 1, Suite 100, Los Angeles, California 90021. *See* la.shopify.com. The location appears set up to help its merchant customers start, run, and scale their businesses.

18. In addition, Shopify has incorporated the majority of its material subsidiaries in the United States, which includes Shopify Holdings and Shopify

USA—both of which are incorporated in Delaware.

Shopify's Business Relationship with MCS

19. MCS is an online computer hardware and software retailer. MCS's business is conducted through its website: www.mychoicesoftware.com, which is hosted on Shopify's e-commerce platform.

20. In April 2015 MCS personnel contacted Shopify about potentially migrating MCS's e-commerce platform to Shopify because of a major outage with MCS's then existing vendor.

21. Through a series of emails and phone calls, MCS made the decision to and did transition its e-commerce platform to Shopify in May 2015. During these exchanges MCS personnel explained the unique nature of MCS's business, which included downloadable products and keeping track of customers software licenses.

22. On January 6, 2017, Loren Padelford, the Vice President and General Manager of Revenue at Shopify, Inc. emailed Nathan Mumme (CEO of MCS) discussing the changes to Shopify Plus (Shopify's enterprise e-commerce platform tailored for larger brands) and its pricing model.

23. On January 16, 2017, Padelford visited MCS's offices in Orange County and met with MCS management to discuss Shopify Plus's new pricing model and contract, and how it would affect MCS as an existing customer and on information and belief, a top Shopify store. During the meeting Padleford represented that as a long-standing and high-performing customer, MCS would receive certain business incentives for continuing to use Shopify as its e-commerce platform. Padleford's purpose for having an in-person meeting with MCS at its Orange County office was to encourage and ensure a continued business relationship between Shopify and MCS.

24. On June 1, 2017, the parties executed the Shopify Plus Agreement that was discussed during the in person meeting between Padleford and MCS management.

TaskUs's Involvement and its Contacts with California

25. According to Shopify's 2023 Annual Report, Shopify International Limited ("Shopify International") is a wholly owned subsidiary that is incorporated in Ireland.

26. On April 21, 2016, Shopify International entered into a Master Services Agreement ("MSA") with TaskUs for customer service work. Although entered into by Shopify International, the services to be provided by TaskUs under the MSA were for the benefit of Shopify and Shopify's merchants, such as MCS.

27. Notably, at the time it entered into the MSA, TaskUs was headquartered in Santa Monica, California. This is reflected by the addresses used in the MSA.

28. The MSA also directed payment remittance to a California bank.

29. On information and belief, TaskUs was still headquartered in Santa Monica, California at the time of the data breach incident referred to herein.

30. While performing customer service work for Shopify, and by extension, its customers, TaskUs had access to Shopify's internal network, which hosted MCS's online store.

31. Shopify did not implement adequate security measures or access controls over TaskUs to ensure the security of information and data contained in Plaintiff's online store.

32. TaskUs did not implement adequate security measures or access controls with respect to its employees.

33. While performing their service functions on the Shopify platform on TaskUs computers at TaskUs facilities, defendant TaskUs employees accessed and/or allowed other defendants, including but not limited to defendant Heinrich, to access Plaintiff's online store's cloud-based protected computer and network without Plaintiff's knowledge or authorization.

34. Plaintiff is informed and believes that employees of defendant TaskUs,

defendant Heinrich, and others paid and/or received incentives (including payments in the form of cryptocurrency and/or false positive reviews) in exchange for access to Plaintiff's protected computer and network on the Shopify platform.

35. On September 18, 2020 Padleford notified MCS that its online store was compromised through a data breach.

36. Shopify limited the information it was willing to disclose to Plaintiff about the breach. Shopify claimed this was due to an ongoing criminal investigation.

37. Plaintiff eventually obtained a security incident report from Shopify with an event log. The event log indicated on July 16, 2020 an unknown person(s) installed a "private application" on MCS's protected computer and network on the Shopify platform. The application issued a command to export all of MCS's customer and order reports (423,179 records). Three hours later the "private application" was uninstalled and removed from MCS's protected computer and network on the Shopify platform.

38. As known by Shopify during the course of forming its business relationship with MCS, MCS stores its downloadable product key numbers as part of its customer order records.

39. The files breached included the customer order records containing the product keys purchased and inventoried by MCS to value over $100 million.

40. Plaintiff is informed and believes that defendant TaskUs employees and/or Heinrich installed the "private application" to steal, use and sell the stolen merchant data, including but not limited to the highly valuable product keys.

41. Plaintiff is informed and believes that defendant Heinrich and defendant TaskUs employees illegally sold and/or caused to be sold MCS's stolen merchant data, including its product keys, on illicit marketplaces, including the dark web. Plaintiff is informed and believes that at least one dark web vendor was offering to sell MCS' customer order records, including product keys, belonging to

MCS.

42. MCS also received reports, and continues to receive reports, from its customers post data breach whose product keys are no longer working. As a result, MCS has had to replace non-working product keys at its own expense and/or issue refunds for its customers and, upon information and belief, all of its product keys have been compromised. Because the product keys stopped working for its customers MCS has also suffered reputational damages and loss of future revenue. MCS is informed and believes that the product keys issued by MCS to its customers were used or sold by Heinrich and TaskUs employees in connection with the breach.

43. On February 19, 2021 defendant Heinrich was indicted by a federal grand jury in connection with the Shopify data breach for stealing data from certain targeted Shopify vendors. The indictment describes Heinrich's conduct and the conduct of the non-indicted co-conspirators. While majority of the criminal case is under seal, Heinrich plead guilty on February 25, 2022.

44. Plaintiff is informed and believes that defendant Heinrich's indictment includes and relates to conduct involving the theft, sale and use of MCS's merchant data, including but not limited to, its product keys, from MCS's protected computer and network on the Shopify platform.

45. Plaintiff is informed and believes that the unnamed "co-conspirators" described in the indictment were employees of defendant TaskUs.

FIRST CLAIM FOR RELIEF
BREACH OF WRITTEN CONTRACT
(AGAINST SHOPIFY, INC.)

46. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

47. There is a valid and enforceable contract between MCS and Shopify, Inc., namely, the Shopify Plus Agreement. A copy of the Shopify Plus Agreement has been filed conditionally under seal by Shopify in this action as ECF No. 28-3.

48. While the Shopify Plus Agreement does contain a forum selection clause designating Canada, the forum selection clause is invalid and/or unenforceable because it (i) contravenes California's strong legislative, statutory, and judicial public policies pertaining to privacy rights and data breaches, (ii) runs contrary to fundamental fairness by, among other things, discouraging the pursuit of legitimate claims by way of a remote alien forum and failing to provide notice of the remote forum, and (iii) is tantamount to a pre-trial jury waiver.

49. Sections 1 and 8.5 of the Shopify Plus Agreement incorporate Shopify, Inc.'s Privacy Policy, which it states "will govern the use and storage of, and access to, personal information" of MCS and MCS's customers.

50. The Shopify Privacy Policy, is available at www.shopify.com/legal/privacy. Attached as **Exhibit A** is a true and correct copy of Shopify, Inc.'s Privacy Policy.

51. On information and belief, the Shopify Privacy Policy that was in place at the time of the data breach is identical and/or substantially similar to the current Privacy Policy in Exhibit A.

52. In the Shopify Privacy Policy, Shopify, Inc. states that its "teams work tirelessly to protect your information, and to ensure the security and integrity of our platform" and that Shopify has "independent auditors assess the security of [its] data storage and systems."

53. MCS performed each and every promise and condition required to be performed by it pursuant to the Shopify Plus Agreement.

54. Defendant Shopify, Inc. materially breached its obligations to MCS under the Shopify Plus Agreement as alleged herein, including by failing to adequately protect and safeguard MCS's information by disregarding standard information security principles, despite obvious risks; by allowing unmonitored and unrestricted access to unsecured information; by failing to provide adequate supervision and oversight of the information with which it was entrusted, in spite

of the known risk and foreseeable likelihood of compromise and misuse, which permitted TaskUs employees to gather MCS's information and intentionally disclose it to others without consent, resulting in its unauthorized and illegal misuse.

55. As a direct and proximate result of defendant Shopify, Inc.'s breaches, MCS has been and will continue to be damaged by the unauthorized disclosure of MCS's confidential merchant data, including the sale of such information on illicit marketplaces like the dark web.

SECOND CLAIM FOR RELIEF
BREACH OF THIRD PARTY BENEFICIARY CONTRACT
(AGAINST TASKUS)

56. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

57. There is a valid and enforceable contract between Shopify International Limited (and its affiliate Shopify) and TaskUs, namely, the Master Services Agreement dated April 21, 2016. A copy of the Master Services Agreement has been filed conditionally under seal by Shopify in this action as ECF No. 28-5.

58. The Master Services Agreement was expressly made for the benefit of Shopify's customers, which includes MCS, as it was MCS's confidential information that TaskUs agreed to process and protect.

59. TaskUs knew that, if it were to breach the Master Services Agreement, MCS would be harmed.

60. TaskUs breached its third-party beneficiary contract with Shopify when it failed to use reasonable data security measures that would have prevented the data breach.

61. As foreseen and contemplated in the Master Services Agreement, MCS was harmed by TaskUs's failure to use reasonable data security measures to

protect MCS's confidential information.

62. As a direct and proximate result of Defendant TaskUs's breaches, MCS has been and will continue to be damaged by the unauthorized disclosure of MCS's confidential merchant data, including the sale of such information on illicit marketplaces like the dark web.

THIRD CLAIM FOR RELIEF
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT UNDER 18 U.S.C. § 1030 (AGAINST TASKUS)

63. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

64. In violation of 18 U.S.C. § 1030(a)(4), Defendant TaskUs, through its employees, knowingly and with intent to defraud, accessed Plaintiff's protected computer without authorization and/or exceeded authorized access and by means of such conduct furthered the intended fraud and obtained value.

65. Defendant TaskUs's conduct caused loss to one or more persons during any one year period aggregating at least $5,000 in value, as set forth in 18 U.S.C. § 1030(c)(4)(A)(i)(I).

66. Defendant TaskUs's conduct caused damage affecting 10 or more protected computers during any 1-year period, as set forth in 18 U.S.C. § 1030(c)(4)(A)(i)(VI).

67. Defendant TaskUs, through its employees, installed a malicious private application on Plaintiff's protected computer.

68. Defendant TaskUs issued a command through the malicious private application to extract and caused to be extracted protected MCS merchant data.

69. Defendant TaskUs then deleted the malicious private application attempting to conceal its use.

70. Defendant TaskUs then provided MCS's confidential merchant data, which included its product keys, to Defendant Heinrich and/or other third parties in

exchange for money and/or other consideration. As a result, MCS's confidential merchant data, including the product keys is being unlawfully sold on illicit marketplaces, including on the dark web.

71. As a result of Defendant TaskUs's unauthorized access to MCS's protected computer and extraction of protected data MCS has been damaged. The losses to MCS well exceed $5,000. The total value of the product keys exceeds $100 million and all product key numbers were contained in the order records unlawfully accessed and taken. MCS has been forced to refund customers and/or replace several software product keys that no longer work, at its own expense, due to having been compromised and unlawfully sold.

72. MCS is also entitled to injunctive relief and any other equitable relief that the Court deems just and proper.

FOURTH CLAIM FOR RELIEF
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT UNDER 18 U.S.C. § 1030
(AGAINST HEINRICH)

73. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

74. In violation of 18 U.S.C. § 1030(a)(4), Defendant Heinrich knowingly and with intent to defraud, accessed Plaintiff's protected computer without authorization and/or exceeded authorized access and by means of such conduct furthered the intended fraud and obtained value.

75. In violation of 18 U.S.C. § 1030(b), Defendant Heinrich conspired to commit an offense in violation of 18 U.S.C. § 1030(a)(4) with Defendant TaskUs.

76. Defendant Heinrich's conduct caused loss to one or more persons, including MCS, during any one year period aggregating at least $5,000 in value, as set forth in 18 U.S.C. § 1030(c)(4)(A)(i)(I).

77. Defendant Heinrich's conduct caused damage affecting 10 or more protected computers during any 1-year period, as set forth in 18 U.S.C. §

1030(c)(4)(A)(i)(VI).

78. Defendant Heinrich bribed TaskUs employees to install a malicious private application on Plaintiff's protected computer.

79. Defendant TaskUs issued a command through the malicious private application to extract and caused to be extracted protected MCS merchant data.

80. Defendant TaskUs then deleted the malicious private application attempting to conceal its use.

81. Defendant TaskUs then provided MCS's confidential merchant data to Defendant Heinrich and/or other third parties in exchange for money and/or other consideration. As a result, MCS's confidential merchant data, including the product keys is being unlawfully sold on illicit marketplaces, including on the dark web.

82. As a result of Defendant Heinrich's unauthorized access to MCS's protected computer and extraction of protected data MCS has been damaged. The losses to MCS well exceed $5,000. The total value of the product keys exceeds $100 million and all product key numbers were contained in the order records unlawfully accessed and taken. MCS has been forced to refund customers and/or replace several software product keys that no longer work, at its own expense, due to having been compromised and unlawfully sold.

83. MCS is also entitled to injunctive relief and any other equitable relief that the Court deems just and proper.

FIFTH CLAIM FOR RELIEF
CALIFORNIA COMPUTER DATA ACCESS AND FRAUD ACT CAL. PENAL CODE § 502 (AGAINST TASKUS)

84. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

85. Defendant TaskUs, through its employees, knowingly and without permission provided or assisted in providing a means of accessing and/or accessed

or caused to be accessed MCS's computer, computer system, or computer network in violation of Penal Code §502(c)(6)-(7).

86. Defendant TaskUs knowingly accessed and without permission altered, damaged, deleted, destroyed, or otherwise used Plaintiff's data, computer, computer system, or computer network in order to wrongfully control or obtain money, property, data belonging to MCS, including its customer order reports containing its highly valuable software product keys, in violation of Penal Code §502(c)(1)(B).

87. Defendant TaskUs knowingly accessed and without permission took, copied, or made use of merchant data, including its software product keys, from MCS's computer, computer system, and/or computer network in violation of Penal Code §502(c)(2).

88. Defendant TaskUs knowingly introduced a computer contaminant into a computer, computer system, or computer network by installing, commanding and deleting a malicious private application on MCS's protected computer and network in violation of Penal Code §502(c)(8).

89. As a result of Defendant TaskUs's knowing access without permission to MCS's protected computer and extraction of protected data MCS is entitled to compensatory damages, injunctive relief, and any other equitable relief that the Court deems just and proper pursuant to Penal Code §502(e)(1).

90. MCS is also entitled to reasonable attorneys' fees pursuant to Penal Code §502(e)(2).

91. Because Defendant TaskUs willfully violated this statute, and its actions were oppressive, fraudulent and malicious, Plaintiff is entitled to punitive or exemplary damages under California Penal Code § 502(e)(4).

///

///

SIXTH CLAIM FOR RELIEF
CALIFORNIA COMPUTER DATA ACCESS AND FRAUD ACT
CAL. PENAL CODE § 502
(AGAINST HEINRICH)

92. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

93. Defendant Heinrich knowingly used Plaintiff's data, computer, computer system, or computer network in order to wrongfully control or obtain money, property, or data belonging to MCS, including its customer order reports containing its highly valuable software product keys, in violation of Penal Code §502(c)(1)(B).

94. Defendant Heinrich, knowingly and without permission provided or assisted in providing a means of accessing and/or accessed or caused to be accessed MCS's computer, computer system, or computer network in violation of Penal Code §502(c)(6).

95. Defendant Heinrich knowingly introduced a computer contaminant into a computer, computer system, or computer network by installing, commanding and deleting a malicious private application on MCS's protected computer and network in violation of Penal Code §502(c)(8).

96. As a result of Defendant Heinrich's knowing access without permission to MCS's protected computer and extraction of protected data MCS is entitled to compensatory damages, injunctive relief, and any other equitable relief that the Court deems just and proper pursuant to Penal Code §502(e)(1).

97. MCS is also entitled to reasonable attorneys' fees pursuant to Penal Code §502(e)(2).

98. Because Defendant Heinrich willfully violated this statute, and the actions were oppressive, fraudulent and malicious, Plaintiff is entitled to punitive or exemplary damages under California Penal Code § 502(e)(4).

///

SEVENTH CLAIM FOR RELIEF
NEGLIGENCE
(AGAINST THE SHOPIFY DEFENDANTS)

99. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

100. Upon The Shopify Defendants' acceptance and storage of MCS's information in their computer systems and on their networks, Defendants undertook and owed a duty to MCS to, among other things, exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. The Shopify Defendants knew MCS's information was private and confidential, including its customer order records with the product key numbers, and should be protected as private and confidential.

101. The Shopify Defendants breached their duty to MCS to adequately protect and safeguard MCS's information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured information. The Shopify Defendants failed to provide adequate supervision and oversight of the information with which they were entrusted, in spite of the known risk and foreseeable likelihood of compromise and misuse, which permitted TaskUs employees to gather MCS's information and intentionally disclose it to others without consent, resulting in its unauthorized and illegal misuse.

102. As a result of the data breach and Shopify's negligence, MCS has suffered substantial non-economic losses beyond simply associated costs. MCS has spent countless hours responding and addressing the data breach (including, but not limited to, the time involved in evaluating how to redress the stolen and compromised product keys), suffered embarrassment and the risk of embarrassment, suffered the loss of business goodwill, and suffered privacy injuries pertaining to the data breach.

103. As a direct and proximate result of the Shopify Defendants' conduct, MCS has suffered monetary damages in an amount to be proven at trial.

EIGHTH CLAIM FOR RELIEF
NEGLIGENCE
(AGAINST TASKUS)

104. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

105. Upon TaskUs's access to Shopify's internal network, TaskUs undertook and owed a duty to MCS to, among other things, exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. TaskUs knew that Shopify merchant store information, including MCS store information, was private and confidential and should be protected as private and confidential.

106. TaskUs breached its duty to MCS to adequately protect and safeguard MCS's information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured information. TaskUs failed to provide adequate supervision and oversight of the information with which it was entrusted, in spite of the known risk and foreseeable likelihood of compromise and misuse, which permitted its employees to gather MCS's information and intentionally disclose it to others without consent, resulting in its unauthorized and illegal misuse.

107. As a direct and proximate result of TaskUs's conduct, MCS has suffered monetary damages in an amount to be proven at trial.

108. As a result of the data breach and TaskUs's negligence, MCS has suffered also substantial non-economic losses beyond simply associated costs. MCS has spent countless hours responding and addressing the data breach (including, but not limited to, the time involved in evaluating how to redress the stolen and compromised product keys), suffered embarrassment and the risk of embarrassment,

suffered the loss of business goodwill, and suffered privacy injuries pertaining to the data breach.

109. As a direct and proximate result of TaskUs's conduct, MCS has suffered monetary damages in an amount to be proven at trial.

NINTH CLAIM FOR RELIEF
CONVERSION
(AGAINST HEINRICH)

110. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

111. MCS had a right to exclusively possess its merchant data stored on its protected computer and network from MCS's online store.

112. Defendant Heinrich intentionally and substantially interfered with MCS's property by stealing, selling and using Plaintiff's data, including its product keys, unlawfully taken from its online store..

113. As a direct and proximate result of Defendant Heinrich's conversion, MCS has suffered, and will continue to suffer, severe and irreparable damage including, but not limited to, the ability to use and control the use of its merchant data, including its product keys.

114. Because the conversion was the result of a theft MCS is entitled to treble damages, costs of the suit and attorneys' fees.

115. Because Defendant Heinrich's conversion of MCS's property was done with oppression, fraud or malice, Plaintiff is entitled to an award of punitive damages.

TENTH CLAIM FOR RELIEF
RECEIPT OF STOLEN PROPERTY
CAL. PENAL CODE § 496
(AGAINST HEINRICH)

116. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

117. Defendant Heinrich stole, bought, received and sold property belonging to MCS.

118. Defendant Henrich's theft consisted of acts including but not limited to unlawfully accessing, downloading, selling and using MCS's merchant data, including but not limited to its software license key numbers, without MCS's knowledge or permission.

119. As a result of Defendant Heinrich's theft and receipt of MCS's stolen property MCS has been harmed.

120. Defendants Heinrich's illegal theft and receipt of stolen property entitles MCS to an award of treble damages, costs of the suit and attorneys' fees.

ELEVENTH CLAIM FOR RELIEF
UNJUST ENRICHMENT
(AGAINST HEINRICH)

121. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint as if fully set forth herein.

122. Heinrich received and retained a benefit from stealing, selling and using Plaintiff's merchant data unlawfully taken from its online store on the Shopify platform, which caused Heinrich to become unjustly enriched.

123. As a result of Heinrich's conduct, MCS is entitled to receive an award in the amount that Heinrich has been unjustly enriched, in an amount to be proven at trial.

PAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against Defendants as follows:

1. For a compensatory damages;
2. For consequential damages;
3. For an award of punitive damages;
4. For imposition of a constructive trust;
5. For injunctive relief;

6. For restitution;

7. For an accounting;

8. For costs of suit, including reasonable attorneys' fees; and

9. For such other and further relief as the court may deem just and proper.

DATED: March 6, 2023

HANSEN LAW FIRM, P.C.

/s/ Craig Alan Hansen, Esq.
CRAIG ALAN HANSEN
SARAH WAGER
BRUNO TARABICHI
Attorney for Plaintiff
My Choice Software, LLC,
a California limited liability company

DEMAND FOR JURY TRIAL

MCS hereby demands a trial of all claims by jury to the extent authorized by law.

DATED: March 6, 2023

HANSEN LAW FIRM, P.C.

/s/ Craig Alan Hansen, Esq.
CRAIG ALAN HANSEN
SARAH WAGER
BRUNO TARABICHI
Attorney for Plaintiff
My Choice Software, LLC,
a California limited liability company

EXHIBIT A

Privacy Policy

How Shopify handles your data

Updated March 2, 2023

Introduction

In our mission to make commerce better for everyone at Shopify, we collect and use information about you, our

- merchants using Shopify to power your business
- customers who shop at a Shopify-powered business
- partners who develop apps for merchants to use, build stores on behalf of merchants, refer potential entrepreneurs to Shopify, or otherwise help merchants operate or improve their Shopify-powered business
- users of Shopify apps and services like Shop or Shop Pay
- visitors to Shopify’s websites, or anyone contacting Shopify support

This Privacy Policy will help you better understand how we collect, use, and share your personal information. If we change our privacy practices, we may update this privacy policy. If any changes are significant, we will let you know (for example, through the Shopify admin or by email).

Our values

Trust is the foundation of the Shopify platform and includes trusting us to do the right thing with your information. Three main values guide us as we develop our products and services. These values should help you better understand how we think about your information and privacy.

Your information belongs to you

We carefully analyze what types of information we need to provide our services, and we try to limit the information we collect to only what we really need. Where possible, we delete or anonymize this information when we no longer need it. When building and improving our products, our engineers work closely with our privacy and security teams to build with privacy in mind. In all of this work our guiding principle is that your information belongs to you, and we aim to only use your information to your benefit.

We protect your information from others

If a third party requests your personal information, we will refuse to share it unless you give us permission or we are legally required. When we are legally required to share your personal information, we will tell you in advance, unless we are legally forbidden.

We help merchants and partners meet their privacy obligations

Many of the merchants and partners using Shopify do not have the benefit of a dedicated privacy team, and it is important to us to help them meet their privacy obligations. To do this, we try to build our products and services so they can easily be used in a privacy-friendly way. We also provide detailed FAQs and documentation covering the most important privacy topics, and respond to privacy-related questions we receive.

Why we process your information

We generally process your information when we need to do so to fulfill a contractual obligation (for example, to process your subscription payments to use the Shopify platform), or where we or someone we work with needs to use your personal information for a reason related to their business (for example, to provide you with a service). Laws in the European Economic Area ("EEA") and in the United Kingdom ("UK") call these reasons "legitimate interests." These "legitimate interests" include:

- preventing risk and fraud
- answering questions or providing other types of support
- helping merchants find and use apps through our app store
- providing and improving our products and services
- providing reporting and analytics
- testing out features or additional services
- assisting with marketing, advertising, or other communications

We only process personal information for these "legitimate interests" after considering the potential risks to your privacy and balancing any risks with certain measures—for example, by providing clear transparency into our privacy practices, offering you control over your personal information where appropriate, limiting the information we keep, limiting what we do with your information, who we send your information to, how long we keep your information, or the technical measures we use to protect your information.

We may also process your personal information where you have provided your consent. In particular, where we cannot rely on an alternative legal basis for processing, where you direct us to transfer information to a third party, where we receive your data from a third party is sourced and it already comes with consent or where we are required by law to ask for your consent (including in the context of some of our sales and marketing activities). At any time, you have a right to withdraw your consent by changing your communication choices, opting out from our communications or by contacting us.

Depending on whether you are a merchant, customer, partner, user or visitor, please refer to our supplemental privacy policies, as relevant, to understand our purposes for processing, categories of recipients and legal basis for processing for each type of personal data.

Your rights over your information

We believe you should be able to access and control your personal information no matter where you live. Depending on how you use Shopify, you may have the right to request access to, correct, amend, delete, port to another service provider, restrict, or object to certain uses of your personal information. We will not charge you more or provide you with a different level of service if you exercise any of these rights. Please note that a number of these rights apply only in certain circumstances, and all of these rights may be limited by law.

If you buy something from or otherwise provide your information to a Shopify-powered store and wish to exercise these rights over information about your purchase or interaction, you need to directly contact the merchant you interacted with. We are a processor and process information on their behalf. We will of course help our merchants to fulfill these requests to the extent required by law, such as by giving them the tools to do so and by answering their questions.

If you are a merchant, partner, Shop user, Shopify employee, website visitor or other individual that Shopify has a direct relationship with, please submit your data subject request through our online portal. Please note that if you send us a request relating to your personal information, we have to make sure that it is you before we can respond. In order to do so, we may use a third party to collect and verify identification documents. Further information about rights available to US residents can be found below under the header "United States Regional Privacy Notice".

If you are not happy with our response to a request, you can contact us to resolve the issue. If you are located in the EEA or UK, you also have the right to lodge a complaint with your local data protection or privacy authority at any time.

Finally, because there is no common understanding about what a "Do Not Track" signal is supposed to mean, we don't respond to those signals in any particular way.

Where we send your information

We are a Canadian company, but we work with and process data about individuals across the world. To operate our business, we may send your personal information outside of your state, province, or country, including to the United States. This data may be subject to the laws of the countries where we send it. We take steps to protect your information when we send your information across borders.

Depending on whether you are a merchant, customer, partner, user or visitor, please refer to our supplemental privacy policies, as relevant.

Transfers outside of Europe and Switzerland

If you are located in the EEA, the UK, or Switzerland, your personal information is controlled by our Irish affiliate, Shopify International Ltd. Your information is then sent to other Shopify locations and to service providers who may be located in other regions, including Canada (where we are based) and the United States. When we send your personal information outside of the EEA, UK or Switzerland, we do so in accordance with applicable law.

If you are in the EEA, the UK, or Switzerland, when we send your personal information to Canada it is protected under Canadian law, which the European Commission has found adequately protects your information. If we then send this personal information outside of Canada (for example, when we send this information to our Subprocessors), this information is protected by contractual commitments that are comparable to those provided in the Standard Contractual Clauses.

Finally, while we do what we can to protect your information, we may at times be legally required to disclose your personal information (for example, if we receive a valid court order). For information about how we respond to such orders, please review our Guidelines for Legal Requests.

How long do we retain your information

We will retain your personal data only for as long as necessary to fulfill the purposes for which we have collected it. To determine the appropriate retention period, we consider the amount, nature and sensitivity of your personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means and the applicable legal requirements. We will also retain and use your personal information to the extent necessary to comply with our legal obligations, resolve disputes and enforce our policies. If you stop using our services or if you delete your account with us, we will delete your information or store your information in an aggregated and anonymized format.

Depending on whether you are a merchant, customer, partner, user or visitor, please refer to our supplemental privacy policies, as relevant, for further details on the retention of your personal information.

Our use of Machine Learning

One of the ways in which we are able to help merchants using Shopify is by using techniques like "machine learning" (some laws, including certain EEA and UK laws, may refer to this as "automated decision-making") to help us improve our services. When we use machine learning, we either: (1) still have a human being involved in the process (and so are not fully automated); or (2) use machine learning in ways that don't have legal or similarly significant effects (for example, reordering how apps might appear when you visit the app store).

How we protect your information

Our teams work tirelessly to protect your information, and to ensure the security and integrity of our platform. We also have independent auditors assess the security of our data storage and systems that process financial information. However, we all know that no method of transmission over the Internet, and method of electronic storage, can be 100% secure. This means we cannot guarantee the absolute security of your personal information. You can find more information about our security measures at https://www.shopify.com/security.

How we use “cookies” and other tracking technologies

We use cookies and similar tracking technologies on our website and when providing our services. For more information about how we use these technologies, including a list of other companies that place cookies on our sites, a list of cookies that we place when we power a merchant’s store, and an explanation of how you can opt out of certain types of cookies, please see our Cookie Policy.

How you can reach us

If you would like to ask about, make a request relating to, or complain about how we process your personal information, please contact Shopify Support, or mail us at one of the addresses below. If you would like to submit a legally binding request to demand someone else’s personal information (for example, if you have a subpoena or court order), please review our Guidelines for Legal Requests.

If you are a merchant, partner, Shop user, Shopify employee, website visitor or other individual that Shopify has a direct relationship with and you are located in the EEA or UK, Shopify International Ltd is the controller of your personal data. If you buy something from or otherwise provide your information to a Shopify-powered store, the merchant is your data controller and we are acting as a processor on their behalf.

If you have questions about how a merchant or store processes your personal information, you should contact the merchant or visit their privacy policy.

Shopify Inc.
ATTN: Chief Privacy Officer
151 O’Connor Street
Ground floor,
Ottawa, ON K2P 2L8
Canada

If you are located in the EEA, the UK, the Middle East, South America, or Africa:

Shopify International Ltd.
Attn: Data Protection Officer
c/o Intertrust Ireland
2nd Floor 1-2 Victoria Buildings
Haddington Road
Dublin 4, D04 XN32
Ireland

If you are located in Asia, Australia, or New Zealand:

Shopify Commerce Singapore Pte. Ltd.
Attn: Data Protection Officer
77 Robinson Road,
#13-00 Robinson 77,
Singapore 068896

United States Regional Privacy Notice

This United States Regional Privacy Notice ("US Notice") supplements our Privacy Policy and all supplemental privacy policies on www.shopify.com (together, the "Shopify Privacy Policies").

This US Notice is for individuals residing in certain US states and is designed to help you better understand how we collect, use, and disclose your personal information and, depending on how you use Shopify and where you reside, how to exercise available rights under various applicable privacy laws in the US, specifically the California Consumer Privacy Act, the Colorado Privacy Act, the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act (collectively, the "US Privacy Laws").

What information we collect and share about you

To provide our apps and services to you, we must process information about you, including personal information.

We do not "sell" your personal information as that term is defined under US Privacy Laws.

Here is a summary of the categories of personal information we may have collected about you over the past 12 months and with whom we may have disclosed that information to, depending on how you use Shopify.

Categories of personal information collected	Recipients of personal information

• Identifiers, including name, email address, mailing address, phone number;
• Personal information categories listed in the California Customer Records statute, including name, mailing and billing address, phone number, credit or debit card information;
• Commercial information, including products you purchase, place in your shopping cart, favorite or review (if you are a customer) and information you provide us about you and your business (if you are a merchant);
• Photos and videos, which may include face imagery, if you choose to provide them.
• Internet or other electronic network activity information, including information regarding the device and browser you use, network connection, IP address, and how you browse through our apps and sites;
• Geolocation data, including your mailing and billing address;
• Inferences, or information derived from other personal information about you, which could include your preferences, interests, and other information used to personalize your experience;
• Other information you provide; and
• Sensitive personal information, which may include:
  • Government-issued identifiers, including social security, driver's license, state identification card, or passport number;
  • Your account access credentials (such as account log-in, financial account, debit or credit card number in combination with any required security access code, password, or credentials allowing access to an account);
	• Companies who help us provide you with our services, including cloud storage providers, payment processors, fulfillment partners, security vendors, email providers, marketplaces and data analytics vendors;
	• Advertisers and marketing vendors;
	• Merchants whose shops you visit or make purchases from;
	• Partners who provide a range of services to merchants, such as by developing apps or themes for use by merchants, serving as an affiliate that refers potential merchants to us, or helping merchants build or manage stores;
	• Law enforcement or other third parties in connection with legal requests, to comply with applicable law or to prevent harm.

• Your device's precise location (if you are a Shop App user, but only when you allow Shop to access this information); • Information you voluntarily disclose that may reveal certain characteristics about you such as your racial or ethnic origin or sexual orientation • The contents of email messages in the email inboxes that you connect to your Shop account, and information from email messages you transfer to the app to be included in your order history (if you use Shop).	

Why we collect and share your Personal Information

We use and share your personal information for the purposes set out in the Shopify Privacy Policies. For categories of sensitive personal information that we collect, we only use or disclose such information either with your specific consent when required, or as otherwise permitted by law.

Sources of Personal Information

To make commerce better for everyone at Shopify, we collect and use personal information provided by:

- You: We collect the information you provide when you use our platform, including when you sign up for Shopify as a merchant, visit a Shopify-powered store, fill in order information, visit one of Shopify's websites or contact Shopify support. We collect account and payment information you provide to us (including information about your business if you are a merchant), Shopify stores or items you save to favorites, purchases you make, reviews you post, and how you otherwise interact or communicate with stores or other users on our apps or services. We also collect information about how you browse through our apps and sites, including search terms you may enter.
- Your device(s): We collect information from and about the devices you use, including computers, phones, and other web-connected devices you use to access our apps or services, and we combine this information across different devices you use.
- Third parties: We receive information from partners who help us provide you with our services including the following:
  - Email providers. If you use the Shop App and you connect your third party inboxes, such as Gmail or Outlook (according to their terms and policies and as permitted by applicable law), we receive information to identify shopping-related emails and display within Shop information about specific orders you have made, stores you have engaged with in the past, and other related information.
  - Service Providers. We receive information from our service providers, who help us provide services to our merchants, like reviewing accounts for fraud or other concerns.
  - Marketplaces. If you use the Shop App, we receive information about purchases you have made from other marketplaces or platforms, such as Amazon, that you choose to connect through Shop. This information helps us to provide and improve Shop, to personalize your experience using our apps and services, and to determine if you are eligible for specific offers or payment methods.
  - Subprocessors. We work with third party subprocessors for cloud hosting, content delivery, data analysis, internal logging, fulfillment services and email transmission, among others, to provide you with our services. For more information, see Shopify's subprocessors.
  - Analytics and cookie providers. We receive information through our use of cookies, social plugins (such as the Facebook "like" button), pixels and tags for business purposes, such as providing information to help measure how users interact with our website content. For more information about how we use these technologies, see our Cookie Policy.

How long we keep your information

Because we need your personal information to provide Shopify services, we generally keep your personal information, including sensitive personal information, while you use Shopify products or services or until you tell us to delete your information. We may also keep personal information to comply with legal obligations or protect our or other's interests.

If you are a merchant operating a Shopify-powered store, and you close the store, stop paying your subscription fees, or we terminate your account, we retain store information for two years before we begin the deletion process.

When you visit or make a purchase from a merchant's Shopify-powered store, we act as a service provider or processor for the merchant, and the merchant, not Shopify, decides how long your information is retained.

Your rights over your information

Depending on where you live, how you use Shopify, and subject to certain exceptions, you may have some or all of the following rights:

- Right to Know: The right to request that we disclose to you the personal information we collect, use, or disclose about you, and information about our data practices.
- Right to Request Correction: The right to request that we correct inaccurate personal information that we maintain about you.
- Right to Request Deletion: The right to request that we delete personal information that we have collected about you.

To exercise your rights, including the "right to know" and "right to delete," please submit a request through our online portal. If you use Shop or Shop Pay, please visit https://shop.app/opt-out for instructions on how to request deletion of your information.

If you have visited or made a purchase from a merchant's Shopify-powered store, please contact the specific merchant directly. If you make a request to us, we will forward your request to the relevant merchant.

Please note that to protect your information and the integrity of our products and services, we may need to verify your identity before processing your request. In some cases we may need to collect additional information to verify your identity, such as your email address or a government issued ID.

Under US Privacy Laws, you may also designate an authorized agent to make these requests on your behalf. If you use an authorized agent to submit a request, we may need to collect additional information, such as a government issued ID, to verify your identity before processing your request to protect your information.

For information on the CCPA requests we have received, please see here. In certain states, you may have the right to appeal our decision regarding a request related to these rights. If you wish to appeal a decision, please contact Shopify Support.

We will not discriminate against you for exercising any of these rights.

How you can reach us

If you would like to ask about or have concerns about how we process your personal information, please contact Shopify Support. If you want to make a request relating to your personal information, please contact us using the methods set out in the section immediately above.

Investors

Press and Media

Partners

Affiliates

Legal

Service status

Support

Merchant support

Help center

Hire an Expert

Shopify Community

Shopify Events

Developers

Shopify.dev

API documentation

Dev Degree

Shopify Plus

Shopify Fulfillment Network

Linkpop

Hydrogen and Oxygen

Commerce Components

Global impact

Sustainability

Social impact

Build Black

Build Native

Research

Solutions

Online store builder

Website builder

Ecommerce website

USA

Terms of Service

Privacy Policy

Sitemap